1. Contact Information

Department of State Privacy Coordinator
Sheryl Walter
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: 11/1/2012

(b) Name of system: Integrated Automated Fingerprint Identification System

(c) System acronym: DS IAFIS

(d) IT Asset Baseline (ITAB) number: 4516

(e) System description (Briefly describe scope, purpose, and major functions):

The Diplomatic Security Integrated Automated Fingerprint Identification System (DS IAFIS) is a DS General Support System that provides DS Agents access to the national fingerprint and criminal history system (IAFIS) maintained by the FBI. IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. As a result of submitting fingerprints electronically, the DS Agents receive electronic responses to criminal ten-print fingerprint submissions within two hours and within 24 hours for civil fingerprint submissions.

Being able to perform live criminal fingerprint checks is a critical component of the Diplomatic Security Service (DSS) Agent Visa Fraud domestically. Additionally, Procurement Shared Services (PSS) performs civil checks as part of the employee background clearance process.

(f) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): N/A

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

DS IAFIS collects information on employees, possible employees, criminals, suspects to a crime, or other individuals undergoing background checks and criminal investigations, for the purpose of determining whether they have a criminal record.
Information collected includes:

- Name
- Date of Birth
- Place of birth
- Social Security number
- Employment information
- Address
- Fingerprints
- Physical description (height, weight, hair/eye color, tattoos and other markings, etc.)
- Arrest record

b. How is the information collected?

DS IAFIS users obtain fingerprint information (ten-print and rolls) through Cross Match fingerprint scanners and manually enter text information into the Cross Match software application, which is installed locally on authorized workstations.

Cross Match Technologies, Inc. is a leading provider of high-quality interoperable biometric identity management systems, applications and services. Their systems have been deployed to several US Federal Government institutions such as US-VISIT immigration program and Office of Personnel Management (OPM). Cross Match offers multimodal capture capabilities for fingerprints to create Electronic Biometric Transmission Specification (EBTS)-compliant files for submission to local, state, or Federal AFIS systems.

c. Why is the information collected and maintained?

The information is collected and maintained by DS IAFIS for the purpose of performing background checks on individuals, as well as obtaining records in the course of a criminal investigation.

d. How will the information be checked for accuracy?

The users are responsible for ensuring the accuracy of the information. Responses from the FBI have their designated Originating Agency Identification (ORI) numbers and Request Information. The user has to make sure that the request information, ORI and the FBI response are identical to ensure that this is the information regarding the person being checked. Users can also perform a secondary request of the same personnel and determine if the same FBI database information is identical.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to DS IAFIS, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended);
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

DS IAFIS collects the minimum amount of personally identifiable information necessary to complete its mandated function of providing automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments; physical and environmental protection; encryption; access control; personnel security; identification and authentication; contingency planning; media handling; configuration management; boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software); and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

DS IAFIS is used by DS Agents to perform automated fingerprint searches that include:

- a latent searching capability,
- electronic image storage, and
- electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year.

Being able to perform live criminal fingerprint checks is a critical component of DSS Agent Visa Fraud domestically. Additionally, Personnel Security and Suitability (PSS) performs civil checks as part of the employee background clearance process.

b. What types of methods are used to analyze the data? What new information may be produced?

There is no data analysis performed by DS. No new information is created due to the fact that information is only retrieved from the existing FBI IAFIS database.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

DS IAFIS enables searches the FBI's IAFIS database for criminal records and background information which are then used by DS as evidence for arraignments and/or arrests of persons being investigated. The information can also be used by DS to determine the employment eligibility of applicants.

d. Is the system a contractor used and owned system?

DS IAFIS is a government-owned system. However, it is being administered and maintained by the DS/CTO/OPS group which consists of both government and contractor personnel. They also train the DS IAFIS users on site. Only certified Cross Match personnel can work and troubleshoot the DS IAFIS system. The users of the system are federal government employees – diplomatic security agents, and PSS personnel.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Strenuous security controls are in place to ensure the protection of the PII used by DS IAFIS, and to negate the threat of function creep. Information in the system is accessed through the use of a logon ID and password. Logins are recorded so that it is readily identifiable who submitted a request. Each transaction is billed by FBI, creating a record of requests. Requiring users to take privacy awareness training also aids in the negation of function creep.

5. Retention

a. How long is information retained?

NARA has determined that civil fingerprint submissions are to be destroyed when the individual reaches 75 years of age and criminal fingerprints are to be destroyed when the individual reaches 99 years of age.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

There are potential risks any time information is stored indefinitely, simply by virtue of the fact that the probability of an incident increases over time. However, the workstations used for DS IAFIS are not connected to the internet, thereby reducing the risk of accidental spillage. Also, DS IAFIS users must comply with proper use policies and user agreements.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Information from DS IAFIS is only shared within DS, and is limited to search results.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is transmitted via SMTP over a secure connection directly to the FBI, and is only transmitted to the user who requested the information.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

DS IAFIS does not share information with any external organizations, as it simply uses existing information from the FBI's IAFIS database.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

DS IAFIS does not share information outside the Department. It retrieves information from the FBI's database. However, the FBI's privacy policy serves as a safeguard for the information.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

DS IAFIS does not share information outside the Department. It retrieves information from the FBI's database. However, the FBI's privacy policy serves as a safeguard for the information.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

Security Records, STATE-36

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

No, individuals do not have the opportunity and/or right to decline to provide the underlying CHRI information, since this is obtained from criminal justice subjects incident to criminal justice processes.

However, individuals generally do have the opportunity and/or right to decline to provide their fingerprints for noncriminal justice purposes, since the individuals generally may opt to not pursue a noncriminal justice activity which requires a fingerprint check. Individuals who chose to engage in such a noncriminal justice activity do not have an option and/or right to object to the use of channelers for processing the fingerprint checks.

Additionally, notice of this type of collection of information is described in the System of Records Notice (SORN) titled Security Records, STATE-36.

b. Do individuals have the opportunity and/or right to decline to provide information?

Individuals do have the right to decline to provide information. However, declining to provide information can have adverse impacts on background checks, which in cases of prospective employees can affect their ability to obtain employment with the Department.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's records disposition schedule, as defined in Diplomatic Security Records, Chapter 11 (discussed in section 5 of this PIA).

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses. In cases of criminal investigation, subjects are made aware of their rights by the agent conducting the investigation. In cases of background checks, the subject is asked for their consent before the database is searched.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

DS IAFIS contains Privacy Act-covered records. Notification and redress are, therefore, rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in section 8 above, and in rules published at 22 CFR 171.31. The procedures instruct the individual how to inquire into the existence of such records, how to request access to their records, and how to request amendment of their record.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. As such, privacy risks associated with notification and redress are minimal.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the system is provided by assigned logon and password and is assigned by DS authorized officials. Each request is numbered and notes the time and place of origin. Access to DS IAFIS is limited to Department of State employees. The following sections of the FAM outline the controls DS IAFIS is utilizing:

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of 3 consecutive invalid access attempts by a user during a 15 minute time frame. After 20 minutes of inactivity a session lock control is implemented at the network layer.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training annually in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risks related to system and information access. Access control lists, which define who can access the system and at what privilege level, are regularly reviewed and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed – or attempted to perform – on an information system.)

DS IAFIS is a government-owned system supported by government and contract employees, who support U.S. Government employees in maintenance of the system.

Contractors who support DS IAFIS are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain U.S. Government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. Contractors involved in the development and/or maintenance of DS IAFIS hardware or software must have at least a SECRET-Level Security Clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), and following and implementing sound policies and procedures from federal, state, local, department and agency entities, are only a few of the safeguards implemented to mitigate the risk to any information technology. DS IAFIS has been designed to minimize risk to privacy data. Please refer to 11(b) for further information.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No technologies in DS IAFIS introduce any privacy risks above those inherent in an IT system.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The C&A for DS IAFIS is currently in Phase I, Risk Management Framework (RMF) Step 2, and system authorization is anticipated to be approved in December 2012.